****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **8/13/2023** | **Moises Castro** |  |

## Client



## Instructions

Submit this completed practices for secure software report. Replace the bracketed text with the relevant information. You must document your process for writing secure communications and refactoring code that complies with software security testing protocols.

* Respond to the steps outlined below and include your findings.
* Respond using your own words. You may also choose to include images or supporting materials. If you include them, make certain to insert them in all the relevant locations in the document.
* Refer to the Project Two Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

[Insert your name here.]

## Algorithm Cipher

AES is a symmetric block cipher used to encrypt data in fixed-size blocks , supporting key sizes of 128, 192, and 256 bits. Utilizing a series of substitution, permutation, and mixing operations, it provides a strong balance between security and performance. Established by the U.S. National Institute of Standards and Technology in 2001, AES has become the de facto standard for securing data across various industries and is often used in conjunction with hash functions like SHA-256 for additional integrity checks. This makes it the best choice for the heavily private data handled in Artemis Financial.

## Certificate Generation

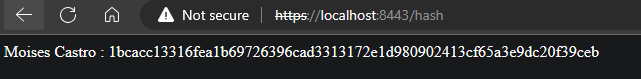
Insert a screenshot below of the CER file.

A screenshot of a computer program

Description automatically generated

## Deploy Cipher

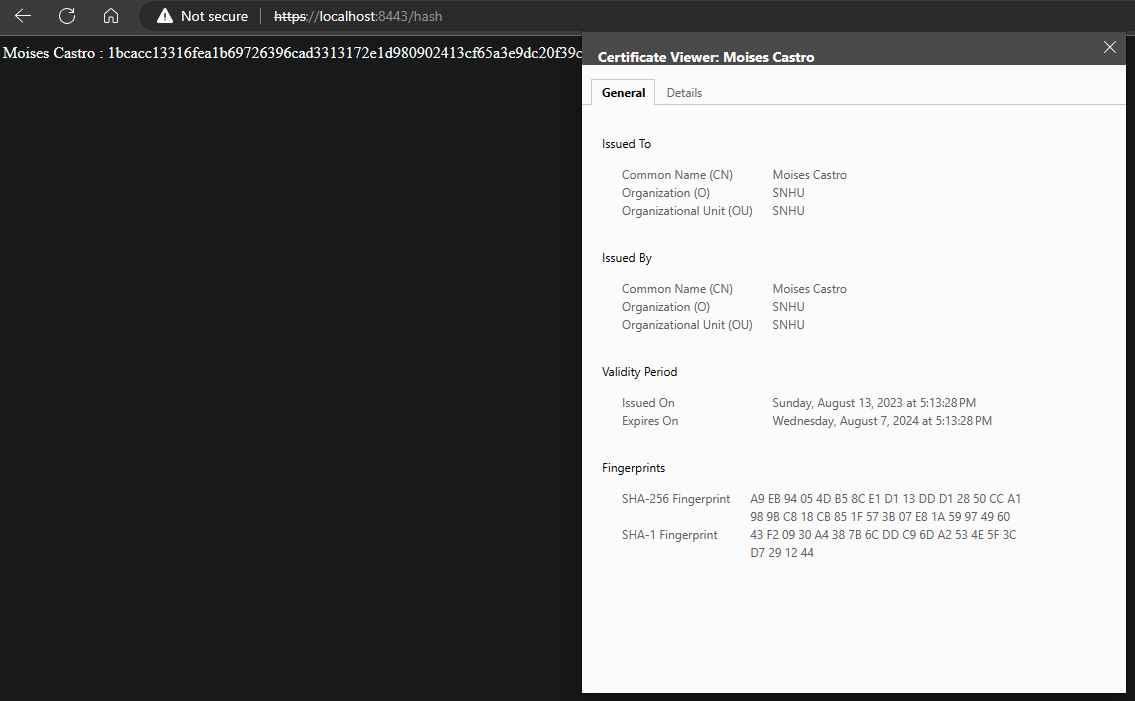
Insert a screenshot below of the checksum verification.



## Secure Communications

Insert a screenshot below of the web browser that shows a secure webpage.

The browser still shows an insecure connection due to the certificate being self signed, I imported it into the browser but still shows an insecure connection.



## Secondary Testing

Insert screenshots below of the refactored code executed without errors and the dependency-check report.

Dependency-check report showed no new vulnerabilities

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

Insert a screenshot below of the refactored code executed without errors.

A screenshot of a computer screen

Description automatically generated

## Summary

The simplicity of the built-in hashing algorithm and using as few external libraries as possible leads to no new vulnerabilities.

## Industry Standard Best Practices

By implementing AES encryption, one of the most widely accepted and secure encryption methods, sensitive information is protected in transit and at rest. Keys are stored securely and managed according to best practices, ensuring that only authorized entities have access to them. By validating all user input and using prepared statements, the application is protected against injection attacks such as SQL Injection. Usage of HTTPS ensures that data is encrypted during transmission, protecting against eavesdropping and man-in-the-middle attacks. By following secure coding practices, sensitive client and financial data are protected, ensuring compliance with regulations such as GDPR and maintaining trust with customers.